Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Apple QuickTime for Windows Denial of Service Vulnerability
  - aspclick.it ACNews Administrative Access Vulnerability
  - Centra Profile Script Insertion Vulnerability
  - Comersus Cross-Site Scripting Vulnerability
  - DameWare Password Disclosure Vulnerability
  - exploitlabs WebcamXP User Redirection and Denial of Service Vulnerability
  - McAfee Internet Security Suite Elevated Privilege Vulnerability
  - **Microsoft Exchange Server Remote Code Execution Vulnerability (Updated)**
  - **Microsoft Internet Explorer Remote Code Execution Vulnerability (Updated)**
  - Microsoft Windows Explorer Preview Pane Script Injection Vulnerability
  - **Microsoft Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities (Updated)**
  - **Microsoft Windows Message Queuing Remote Code Execution Vulnerability (Updated)**
  - **Microsoft Windows Shell Remote Code Execution Vulnerability (Updated)**
  - **Microsoft Windows Kernel Elevation of Privilege and Denial of Service Vulnerabilities (Updated)**
  - **Microsoft Windows License Logging Service Buffer Overflow (Updated)**
  - **Microsoft Word Remote Code Execution and Escalation of Privilege Vulnerabilities (Updated)**
  - Musicmatch Jukebox Elevated Privilege and Cross-Site Scripting Vulnerabilities
  - **NetManage RUMBA Profile Handling Multiple Buffer Overflow (Updated)**
  - OneWorldStore Multiple Vulnerabilities
  - PMSoftware Simple Web Server Buffer Overflow Permits Remote Code Execution
  - RSA Authentication Agent for Web for IIS Cross-Site Scripting Vulnerability
  - Sun Java System Web Server Denial of Service Vulnerability
  - X-Ways WinHex Denial of Service Vulnerability
  - Yager Denial of Service and Remote Code Execution Vulnerabilities
- UNIX / Linux Operating Systems
  - Multiple Apple Vulnerabilities
  - Avaya Labs Libsafe Multi-threaded Process Race Condition Security Bypass
  - FreeBSD 'ifconf()' Function Information Disclosure
  - GNU CPIO CHMod File Permission Modification
  - **GNU Sharutils 'Unshar' Insecure Temporary File Creation (Updated)**
  - **GNU wget File Creation & Overwrite (Updated)**
  - **Hiroyuki Yamamoto Sylpheed Mail Client Remote Buffer Overflow (Updated)**
  - IBM AIX Information Disclosure
  - Oops! Proxy Server Remote Format String
  - IlohaMail Email Message Remote Cross-Site Scripting
  - **ImageMagick Multiple Remote Vulnerabilities (Updated)**
  - **ImageMagick Photoshop Document Buffer Overflow (Updated)**

- **ISC DHCPD Package Remote Format String (Updated)**
- Jamie Cameron Usermin Configuration File Permissions
- Jamie Cameron Webmin Configuration File Permissions
- JunkBuster Vulnerabilities
- **KDE DCOPServer Local Denial of Service (Updated)**
- **LGPL NASM error() Buffer Overflow (Updated)**
- **LibEXIF Library EXIF Tag Structure Validation (Updated)**
- **LibTIFF Buffer Overflows (Updated)**
- **Midnight Commander 'Insert_Text' Buffer Overflow (Updated)**
- moleSoftware GmbH VHCS Input Validation
- Monkey HTTP Daemon Denial of Service & Arbitrary Code Execution
- Multiple Vendors Apple Safari Remote Code Execution
- **Multiple Vendors Perl 'rmtree()' Function Elevated Privileges (Updated)**
- **Multiple Vendors MySQL Database Unauthorized GRANT Privilege (Updated)**
- Multiple Vendors CVS Multiple Vulnerabilities
- **Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows (Updated)**
- Multiple Vendors RSnapshot File Permission Manipulation
- **Multiple Vendors GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service (Updated)**
- **Multiple Vendors Sylpheed MIME-Encoded Attachment Name Buffer Overflow (Updated)**
- **Multiple Vendors Gaim Jabber File Request Remote Denial of Service (Updated)**
- **Multiple Vendors Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service (Updated)**
- Multiple Vendors Sudo VISudo Insecure Temporary File Creation
- **Multiple Vendors XLoadImage Compressed Image Remote Command (Updated)**
- **Vixie Cron Crontab Information Disclosure (Updated)**
- PHP Group Exif Module IFD Nesting Remote Denial of Service
- PHP Group Exif Module IFD Tag Integer Overflow
- **phpMyAdmin 'convcharset' Cross-Site Scripting (Updated)**
- Postgrey Format String
- Salim Gasmi GLD Buffer Overflows & Format Strings
- Sumus Game Server Remote Buffer Overflow
- Sun Solaris libgss Elevated Privileges
- Sun Solaris Network Port Hijacking
- Wilmer van der Gaast Axel 'Conn.c' Remote Buffer Overflow

- Multiple Operating Systems
  - All4WWW-HomePageCreator 'Index.PHP' Arbitrary Code Execution
  - Ariadne CMS Arbitrary Code Execution
  - CityPost Image Cropper/Resizer Cross-Site Scripting
  - CityPost PHP LNKX Cross-Site Scripting
  - CityPost Simple PHP Upload Cross-Site Scripting
  - **Computer Associates BrightStor ARCserve Backup UniversalAgent Remote Buffer Overflow (Updated)**
  - Datenbank PHPBB Module Remote 'Mod.PHP' SQL Injection & Cross-Site Scripting
  - EGroupWare EMail Attachment Information Disclosure
  - eGroupWare Multiple Vulnerabilities
  - F5 BIG-IP User Interface
  - Francisco Burzi PHP-Nuke 'Forwarder' Parameter HTTP Response Splitting
  - GOCR 'ReadPGM' Remote Integer Overflows
  - Gregory Demar Coppermine Photo Gallery 'include/init.inc.php'
  - IBM iSeries AS400 POP3 Server Remote Information Disclosure
  - IBM Lotus Domino Server Malformed POST Request Remote Buffer Overflow
  - IBM OS/400 Incoming Remote Command Denial of Service
  - IBM WebSphere Application Server JSP Source Code Disclosure
  - Kerio MailServer WebMail Remote Denial of Service
  - LG U8120 Mobile Phone MIDI File Remote Denial of Service
  - Matt Kruse CalendarScript Cross-Site Scripting & Information Disclosure
  - Mozilla Suite / Firefox Multiple Vulnerabilities
  - **Mozilla Suite/Firefox JavaScript Lambda Information Disclosure**

(Updated)
- Multiple Vendor TCP Session Acknowledgement Number Remote Denial of Service
- Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service
- Multiple Vendors Squid Proxy Aborted Connection Remote Denial of Service
- MVNForum Search Cross-Site Scripting
- **MySQL CREATE FUNCTION Remote Code Execution Vulnerability (Updated)**
- **MySQL Escalated Privilege Vulnerabilities (Updated)**
- **MySQL udf_init() Path Validation Vulnerability (Updated)**
- MyBloggie Arbitrary Code Execution
- Nash Tech EasyPHPCalendar Cross-Site Scripting & Information Disclosure
- Opera SSL Security Feature False Sense of Security
- Oracle Database Multiple SQL Injection
- Oracle Products Multiple Unspecified Vulnerabilities
- Oracle Applications 'Query/Where' Feature SQL Injection
- Oracle Database 'MDSYS.MD2.SDO_CODE_SIZE' Buffer Overflow
- **PHP Multiple Remote Vulnerabilities (Updated)**
- **PHP 'getimagesize()' Multiple Denials of Service (Updated)**
- phpBB Knowledge Base SQL Injection & Information Disclosure
- PHPBB2 Plus Cross-Site Scripting Vulnerabilities
- Pinnacle Cart 'Index.PHP' Cross-Site Scripting
- Serendipity 'exit.php' Input Validation
- Smartor PHPBB Photo Album Module SQL Injection & Cross-Site Scripting
- SPHPBlog Information Disclosures
- SPHPBlog 'Search.PHP' Cross-Site Scripting
- **OpenOffice Malformed Document Remote Heap Overflow (Updated)**
- Sun JavaMail 'MimeBodyPart.getFileName' Directory Traversal
- Veritas i3 FocalPoint Server Unspecified Error
- Xerox MicroServer SNMP Authentication Bypass

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

Apple QuickTime for Windows 6.5.2	A buffer overflow vulnerability has been reported that could let remote malicious users cause a Denial of Service. This is due to problems handling a malformed GIF image with the maximum depth start value in PictureViewer. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apple QuickTime for Windows Denial of Service Vulnerability CAN-2005-1106	Low	BUGTRAQ:20050413, April 13, 2005
aspclick.it ACNews 1.0	An input validation vulnerability has been reported that could let a remote malicious user execute SQL commands to gain administrative access. This is due to improper input validation in the 'admin/login.asp' script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	aspclick.it ACNews Administrative Access Vulnerability CAN-2005-1149	High	Security Tracker Alert ID: 1013681, April 12, 2005
Centra Centra 7	A vulnerability has been reported that could let a remote malicious user conduct script insertion attacks. This is because of input validation errors in username, first name, and last name fields. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Centra Profile Script Insertion Vulnerability CAN-2005-1104	High	Secunia SA14930, April 13, 2005
Comersus Open Technologies Comersus 4.x	An input validation vulnerability has been reported in the 'curPage' parameter that could let a remote malicious user conduct Cross-Site Scripting attacks. The 'comersus_searchItem.asp' script does not properly validate user-supplied input in the 'curPage' variable. Version 6 is reportedly not affected. A Proof of Concept exploit has been published.	Comersus Cross-Site Scripting Vulnerability CAN-2005-1188	High	OSVDB Reference: 15539, April 12, 2005
DameWare Development DameWare 4.9 and prior - NT Utilities and MiniRemote Control	A vulnerability has been reported that could let a local malicious user obtain passwords. A local user with access to NT Utilities 'DNTUS26' process memory can obtain the username and password. A local user with access to the DameWare MiniRemote Control 'DWRCS' process memory can obtain the applicable username and configuration settings. The 'DWRCC' process is also affected, but can be used to also obtain passwords. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	DameWare Password Disclosure Vulnerability CAN-2005-1166	Medium	Security Tracker Alert ID: 1013725, April 15, 2005
exploitlabs WebcamXP 2.16.468 and prior	Multiple vulnerabilities have been reported in which a remote malicious user could redirect chat users to arbitrary locations and cause a Denial of Service. These vulnerabilities are due to input validation errors in the username field. A fixed version (2.16.478) is available at: http://webcamxp.com A Proof of Concept exploit has been published.	exploitlabs WebcamXP User Redirection and Denial of Service Vulnerability CAN-2005-1189 CAN-2005-1190	Low	Security Tracker Alert ID: 1013753, April 18, 2005
McAfee Internet Security Suite 2005	A file permission vulnerability has been reported that could let a local malicious user can gain elevated privileges or disable the security functions. A local user could modify application files, modify or replace some of the code components with arbitrary code, or move or delete the executable files to cause the security services to fail to startup at reboot. Updates are available through Automatic Update feature. A Proof of Concept exploit has been published.	McAfee Internet Security Suite Elevated Privilege Vulnerability CAN-2005-1107	Medium	iDEFENSE Security Advisory 04.18.05
Microsoft Exchange 2000 Server SP3, 2003, 2003 SP1	A vulnerability has been reported due to an unchecked buffer in the SMTP service that could let a remote malicious user execute arbitrary code. **V1.1: Bulletin updated to reflect a revised "Security Update Information" section for the Word 2003 security update.** Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-021.mspx	Microsoft Exchange Server Remote Code Execution Vulnerability CAN-2005-0560	High	Microsoft Security Bulletin. MS05-021, April 12, 2005 Technical Cyber Security Alert TA05-102A US CERT VU#275193 **Microsoft Security Bulletin. MS05-021**

	Currently we are not aware of any exploits for this vulnerability.			**V1.1, April 14, 2005**
Microsoft Internet Explorer 5.01, 5.5, 6	Multiple vulnerabilities have been reported that include DHTML Object Memory Corruption, URL Parsing Memory Corruption, and Content Advisor Memory Corruption Vulnerability. These vulnerabilities could let remote malicious users execute arbitrary code. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-020.mspx **An exploit script has been published.**	Microsoft Internet Explorer Remote Code Execution Vulnerability CAN-2005-0553 CAN-2005-0554 CAN-2005-0555	High	Microsoft Security Bulletin MS05-020, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#774338 US-CERT VU#756122 US-CERT VU#222050 **Security Focus, 13120, April 12, 2005**
Microsoft Microsoft Windows 2000 Avaya DefinityOne Media Servers, IP600 Media Servers, S3400 Message Application Server, S8100 Media Servers	Microsoft Windows Explorer is prone to a script injection vulnerability. This occurs when the Windows Explorer preview pane is enabled on Windows 2000 computers. If a file with malicious attributes is selected using Explorer, script code contained in the attribute fields may be executed with the privilege level of the user that invoked Explorer. This could be exploited to gain unauthorized access to the vulnerable computer. No vendor workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows Explorer Preview Pane Script Injection Vulnerability CAN-2005-1191	High	Security Focus Bugtraq ID 13248, April 19, 2005
Microsoft Windows 2000 SP 3 and SP4 Windows XP SP 1 and SP2 Windows XP 64-Bit Edition SP1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, Windows 98 SE, and Windows ME	Multiple vulnerabilities have been reported that include IP Validation, ICMP Connection Reset, ICMP Path MTU, TCP Connection Reset, and Spoofed Connection Request. These vulnerabilities could let remote malicious users execute arbitrary code or execute a Denial of Service. Updates available: http://www.microsoft.com/technet/security/bulletin/MS05-019.mspx **A Proof of Concept exploit has been published.**	Microsoft Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities CAN-2005-0048 CAN-2004-0790 CAN-2004-1060 CAN-2004-0230 CAN-2005-0688	Low/ High (High if arbitrary code can be executed)	Microsoft Security Bulletin MS05-019, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#233754 **US-CERT VU#396645**
Microsoft Windows 2000 SP 3 and SP4 Windows XP SP1 Windows XP 64-Bit Edition SP1 Windows 98 and 98 SE	A buffer overflow vulnerability has been reported that could let a remote malicious user execute arbitrary code. **V1.1: Bulletin updated to reflect an updated "Registry Key Verification" section for the Windows XP Service Pack 1 security update.** Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-017.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Message Queuing Remote Code Execution Vulnerability CAN-2005-0059	High	Microsoft Security Bulletin MS05-017, April 12, 2005 **Microsoft Security Bulletin MS05-017 V1.1, April 14, 2005**

Microsoft Windows 2000 SP3 and SP4 Windows XP SP1 and SP2 Windows XP 64-Bit Edition SP 1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, 98 SE, ME	A vulnerability has been reported that could let a remote malicious user execute arbitrary code. This is because of an error in the process to validate which application should load a file. A remote user can convince the Windows Shell to start the HTML Application Host application when that application would not typically be used to process files. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-016.mspx **Exploit scripts have been published.**	Microsoft Windows Shell Remote Code Execution Vulnerability CAN-2005-0063	High	Microsoft Security Bulletin MS05-016, April 12, 2005 US-CERT VU#673051 **Security Focus, 13132, April 13, 2005**
Microsoft Windows 2000 SP3 and SP4 Windows XP SP1 and SP2 Windows XP 64-Bit Edition SP1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, 98 SE, and ME	Multiple vulnerabilities have been reported that include errors in the font, Kernel, Object Management Vulnerability and CSRSS. These are due to input validation and buffer overflow errors. A malicious user could deny service or obtain escalated privileges. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-018.mspx Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Windows Kernel Elevation of Privilege and Denial of Service Vulnerabilities CAN-2005-0060 CAN-2005-0061 CAN-2005-0550 CAN-2005-0551	Low/ Medium (Medium if elevated privileges can be obtained)	Microsoft Security Bulletin MS05-018, April 12, 2005 **US-CERT VU#259197** **US-CERT VU#775933** **US-CERT VU#943749** **US-CERT VU#650181**
Microsoft Windows NT Server 4.0 SP6a, Windows NT Server 4.0 Terminal Server Edition SP6a, Windows 2000 Server SP3 & SP4, Windows 2003, Windows 2003 for Itanium-based Systems Avaya DefinityOne Media Servers; Avaya IP600 Media Servers; Avaya S3400 Message Application Server; Avaya S8100 Media Servers	A buffer overflow vulnerability exists in the License Logging service due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-010.mspx A Proof of Concept exploit has been published. **V 1.2: Bulletin updated to reflect a revised "Mitigating Factors" section for Windows 2000 Server Service Pack 4.**	Microsoft Windows License Logging Service Buffer Overflow CAN-2005-0050	Low/ High (High if arbitrary code can be executed)	Microsoft Security Bulletin, MS05-010, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT VU#130433 Security Focus, Bugtraq ID 12481, April 12, 2005 **Microsoft Security Bulletin, MS05-010 V1.2, February 8, 2005**

Microsoft Word 2000, 2002 Works Suite 2001, 2002, 2003, and 2004 Office Word 2003	A buffer overflow vulnerability has been reported that could lead to remote execution of arbitrary code or escalation of privilege. **V1.1 Bulletin updated to point to the correct Exchange 2000 Server Post-Service Pack 3 (SP3) Update Rollup and to advise on the scope and caveats of workaround "Unregister xlsasink.dll and fallback to Active Directory for distribution of route information."** Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-023.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Word Remote Code Execution and Escalation of Privilege Vulnerabilities CAN-2004-0963 CAN-2005-0558	High	Microsoft Security Bulletin MS05-023, April 12, 2005 US-CERT VU#442567 US-CERT VU#752591 **Microsoft Security Bulletin MS05-023 V1.1, April 14, 2005**
Musicmatch Jukebox 10.00.2047 and prior	Multiple vulnerabilities have been reported that could let a local malicious user gain elevated privileges and let a remote user conduct Cross-Site Scripting attacks. This is because 'MMFWLaunch.exe' does not properly quote path data before calling the CreateProcess() function. Also, the software does not properly filter HTML code from user-supplied input before displaying the input. The vendor has released a fixed version at: http://www.musicmatch.com/download/free/security.htm Currently we are not aware of any exploits for these vulnerabilities.	Musicmatch Jukebox Elevated Privilege and Cross-Site Scripting Vulnerabilities CAN-2005-1167 CAN-2005-1168	High	Hyperdose Security Advisories H2005-04 and H2005-05
NetManage RUMBA 7.3, **7.4**	Multiple buffer overflow vulnerabilities have been reported when RTO and WPA profiles are loaded, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	NetManage RUMBA Profile Handling Multiple Buffer Overflow CAN-2005-0979	Low/ High (High if arbitrary code can be executed)	Security Focus, 12965, April 1, 2005 **Bugtraq, 395705, April 13, 2005**
OneWorldStore OneWorldStore	Multiple vulnerabilities have been reported that could let a remote user conduct cross-site scripting, script insertion and SQL injection attacks. This is due to input validation errors in the "sEmail" parameter in "owContactUs.asp," "bSub" parameter in "owListProduct.asp," "idProduct," and "idCategory" used in a SQL query and the "Name", "Email" and "Comment" parameters in the review form. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	OneWorldStore Multiple Vulnerabilities CAN-2005-1161 CAN-2005-1162	High	Dcrab 's Security Advisory, April 14, 2005
PMSoftware Simple Web Server 1.0.15	A buffer overflow vulnerability has been reported that could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	PMSoftware Simple Web Server Buffer Overflow Permits Remote Code Execution CAN-2005-1173	Low/ High (High if arbitrary code can be executed)	Secunia SA15000, April 19, 2005
RSA Security RSA Authentication Agent for Web for IIS 5.2	A vulnerability has been reported that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to input validation errors in the "postdata" parameter in "/WebID/IISWebAgentIF.dll." Update to version 5.3: http://www.rsasecurity.com/node.asp?id=2807&node_id= A Proof of Concept exploit has been published.	RSA Authentication Agent for Web for IIS Cross-Site Scripting Vulnerability CAN-2005-1118	High	Secunia SA14954, April 15, 2005

Sun Microsystems Sun Java System Web Server (Sun ONE/iPlanet) 6.0 SP7	A vulnerability has been reported that could let remote users cause a Denial of Service. Update to Sun Java System Web Server 6.0 Service Pack 8 or later: http://wwws.sun.com/software/download/products/40968fe6.html Currently we are not aware of any exploits for this vulnerability.	Sun Java System Web Server Denial of Service Vulnerability CAN-2005-1150	Low	Sun Alert ID: 57760, April 13, 2005
X-Ways Software Technology WinHex 12.05 SR-14	A vulnerability has been reported that could let a malicious user cause a Denial of Service with a special filename. The DS, ECX, and ESI register can be overwritten with arbitrary data. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	X-Ways WinHex Denial of Service Vulnerability CAN-2005-1187	Low	Security Tracker Alert ID: 1013727, April 15, 2005
Yager Development Yager 5.24 and prior	Multiple vulnerabilities have been reported that could let a remote malicious user cause a Denial of Service or execute arbitrary code. These vulnerabilities are due to errors in the handling of the nickname field and in the communication handling. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Yager Denial of Service and Remote Code Execution Vulnerabilities CAN-2005-1163 CAN-2005-1164 CAN-2005-1165	Low/ High (High if arbitrary code can be executed)	Luigi Auriemma, April 14, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8	Multiple vulnerabilities have been reported: a Denial of Service vulnerability has been reported in the kernel syscall emulation functionality when handling input parameter lists; a vulnerability has been reported due to an error that allows installation or creation of SUID/SGID scripts, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability has been reported in the 'semop()' system call, which could let a malicious user obtain elevated privileges; a vulnerability has been reported in the 'searchfs()' system call due to an integer overflow, which could let a malicious user obtain elevated privileges; a vulnerability has been reported in the 'setsockopt()' function, which could let a malicious user exhaust available memory resources; a Denial of Service vulnerability has been reported in the 'nfs_mount()' function due to insufficient validation of input values; and a vulnerability has been reported due to an error when parsing certain executable files, which could let a malicious user temporary suspend operations. Upgrades available at: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/ Currently, we are not aware of any exploits for these vulnerabilities.	Multiple Apple Vulnerabilities CAN-2005-0969 CAN-2005-0970 CAN-2005-0971 CAN-2005-0972 CAN-2005-0973 CAN-2005-0974 CAN-2005-0975	Low/ Medium (Medium if elevated privileges can be obtained)	Apple Security Advisory, APPLE-SA-2005-04-15, April 16, 2005
Avaya Labs Libsafe 2.0-16	A race condition vulnerability has been reported when used in multi-threaded applications, which could let a local/remote malicious user bypass security mechanisms. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Libsafe Multi-threaded Process Race Condition Security Bypass CAN-2005-1125	Medium	Security Focus,13190, April 15, 2005

FreeBSD FreeBSD 4.x, 5.x releases prior to 5.4-RELEASE	A vulnerability has been reported in the 'ifconf()' function due to an error when generating a list of network interfaces, which could let a malicious user obtain sensitive information. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:04/ifconf4.patch There is no exploit code required.	FreeBSD 'ifconf()' Function Information Disclosure CAN-2005-1126	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:04, April 15, 2005
GNU cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6	A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions. No workaround or patch available at time of publishing. There is no exploit code required.	CPIO CHMod File Permission Modification CAN-2005-1111	Medium	Bugtraq, 395703, April 13, 2005
GNU sharutils 4.2, 4.2.1	A vulnerability has been reported in the 'unshar' utility due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required.	GNU Sharutils 'Unshar' Insecure Temporary File Creation CAN-2005-0990	Medium	Ubuntu Security Notice, USN-104-1, April 4, 2005 Gentoo Linux Security Advisory, GLSA 200504-06, April 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005 **Fedora Update Notification, FEDORA-2005-319, April 14, 2005**
GNU wget 1.9.1	A vulnerability exists which could permit a remote malicious user to create or overwrite files on the target user's system. wget does not properly validate user-supplied input. A remote user can bypass the filtering mechanism if DNS can be modified so that '..' resolves to an IP address. A specially crafted HTTP response can include control characters to overwrite portions of the terminal window. **SUSE: ftp://ftp.SUSE.com/pub/SUSE** A Proof of Concept exploit script has been published.	GNU wget File Creation & Overwrite CAN-2004-1487 CAN-2004-1488	Medium	Security Tracker Alert ID: 1012472, December 10, 2004 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 **SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005**
Hiroyuki Yamamoto Sylpheed 0.8.11, 0.9.4-0.9.12, 0.9.99, 1.0.0-1.0.2	A buffer overflow vulnerability exists in certain headers that contain non-ASCII characters, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.3.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-303.html	Sylpheed Mail Client Remote Buffer Overflow CAN-2005-0667	High	Security Tracker Alert, 1013376, March 4, 2005 Fedora Update Notification, FEDORA-2005-211, March 15, 2005 RedHat Security Advisory, RHSA-2005:303-05, March 18, 2005 Gentoo Linux Security Advisory, GLSA 200503-26, March 20, 2005

	Gentoo: http://security.gentoo.org/glsa/glsa-200503-26.xml ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.			**SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005** **Turbolinux Security Advisory, TLSA-2005-44, April 19, 2005**
IBM AIX 5.3	A vulnerability has been reported due to a serialization error, which could let a malicious user obtain sensitive information. Fix information available at: http://www-1.ibm.com/support/docview.wss?uid=isg1IY70032 Currently, we are not aware of any exploits for this vulnerability.	IBM AIX Information Disclosure CAN-2005-1176	Medium	IBM Advisory, IY70032, April 14, 2005
Igor Khasilev Oops Proxy Server 1.4.22, 1.5.53	A format string vulnerability has been reported due to insufficient sanitization of user-supplied input before passing to a formatted printing function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently, we are not aware of any exploits for this vulnerability.	Oops! Proxy Server Remote Format String CAN-2005-1121	High	Security Focus, 13172, April 14, 2005
IlohaMail IlohaMail 0.7 .0-0.7.9, 0.8.6-0.8.14	Cross-Site Scripting vulnerabilities have been reported when processing emails due to an input validation error, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	IlohaMail Email Message Remote Cross-Site Scripting CAN-2005-1120	High	Secunia Advisory, April 14, 2005

ImageMagick ImageMagick 5.3.3, 5.3.8, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8 .2-1.1.0 , 5.4.8, 5.5.3 .2-1.2.0, 5.5.4, 5.5.6 .0-20030409, 5.5.6, 5.5.7, 6.0, 6.0.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported in the decoder due to a failure to handle malformed TIFF tags; a remote Denial of Service vulnerability has been reported due to a failure to handle malformed TIFF images; a remote Denial of Service vulnerability has been reported due to a failure to handle malformed PSD files; and a buffer overflow vulnerability has been reported in the SGI parser, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.imagemagick.org/script/download.php? SuSE: ftp://ftp.suse.com/pub/suse RedHat: http://rhn.redhat.com/errata/RHSA-2005-070.html Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for these vulnerabilities.	ImageMagick Multiple Remote Vulnerabilities CAN-2005-0759 CAN-2005-0760 CAN-2005-0761 CAN-2005-0762	Low/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013550, March 24, 2005 Debian Security Advisory, DSA 702-1, April 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:065, April 3, 2005 **Turbolinux Security Advisory, TLSA-2005-47, April 19, 2005**
ImageMagick ImageMagick 6.x	A buffer overflow vulnerability exists in 'coders/psd.c' when a specially crafted Photoshop document file is submitted, which could let a remote malicious user execute arbitrary code. Update available at: http://www.imagemagick.org/www/download.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-26.xml Gentoo: http://security.gentoo.org/glsa/glsa-200501-37.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this	ImageMagick Photoshop Document Buffer Overflow CVE Name: CAN-2005-0005	High	iDEFENSE Security Advisory, January 17, 2005 Ubuntu Security Notice, USN-62-1, January 18, 2005 Debian Security Advisory, DSA 646-1, January 19, 2005 Gentoo Linux Security Advisory, GLSA 200501-26, January 20, 2005 Gentoo Linux Security Advisory, GLSA 200501-37, January 26, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:065, April 3, 2005 **Turbolinux Security Advisory, TLSA-2005-47, April 19, 2005**

	vulnerability.			
ISC DHCPD 2.0.pl5	A format string vulnerability has been reported because user-supplied data is logged in an unsafe fashion, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://security.debian.org/pool/updates/main/d/dhcp/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-212.html** We are not aware of any exploits for this vulnerability.	ISC DHCPD Package Remote Format String CAN-2004-1006	High	Debian Security Advisory, DSA 584-1, November 4, 2004 US-CERT VU#448384 **RedHat Security Advisory, RHSA-2005:212-06, April 12, 2005**
Jamie Cameron Usermin prior to 1.130	A vulnerability has been reported in certain configuration files due to a design error because insecure permissions are assigned, which could let a remote malicious user obtain control of configuration files. Updates available at: http://prdownloads.sourceforge.net/webadmin/usermin-1.130.tar.gz There is no exploit code required.	Usermin Configuration File Permissions CAN-2005-1177	Medium	Security Tracker Alert, 1013723, April 15, 2005
Jamie Cameron Webmin prior to 1.200	A vulnerability has been reported in certain configuration files due to a design error because insecure permissions are assigned, which could let a remote malicious user obtain control of configuration files. Updates available at: http://prdownloads.sourceforge.net/webadmin/usermin-1.130.tar.gz There is no exploit code required.	Webmin Configuration File Permissions CAN-2005-1177	Medium	Security Tracker Alert, 1013723, April 15, 2005
Junkbuster Internet Junkbuster 2.0.1, 2.0.2	Two vulnerabilities have been reported: a vulnerability has been reported in the 'ij_untrusted_url()' function, which could let a remote malicious user modify the configuration; and a vulnerability has been reported due to errors when filtering URLs, which could let a malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200504-11.xml Currently we are not aware of any exploits for these vulnerabilities.	JunkBuster Vulnerabilities CAN-2005-1108 CAN-2005-1109	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory GLSA 200504-11, April 13, 2005
KDE KDE 1.1-1.1.2, 1.2, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2	A Denial of Service vulnerability has been reported in the Desktop Communication Protocol (DCOP) daemon due to an error in the authentication process Upgrade available at: http://www.kde.org/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-22.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-325.html ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/	KDE DCOPServer Local Denial of Service CAN-2005-0396	Low	KDE Security Advisory, March 16, 2005 Fedora Update Notifications, FEDORA-2005-244 & 245, March 23, 2005 RedHat Security Advisory, RHSA-2005:325-07, March 23, 2005 ALTLinux Security Advisory, March 29, 2005 RedHat Security Advisory, RHSA-2005:307-08, April 6,2005 SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005

	2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-307.html SUSE: ftp://ftp.SUSE.com/pub/SUSE **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for this vulnerability.			**SGI Security Advisory, 20050403-01-U, April 15, 2005**
LGPL NASM 0.98.38	A vulnerability was reported in NASM. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted asm file that, when processed by the target user with NASM, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the error() function in 'preproc.c.' Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-20.xml Debian: http://www.debian.org/security/2005/dsa-623 Mandrake: http://www.mandrakesoft.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** A Proof of Concept exploit script has been published.	LGPL NASM error() Buffer Overflow CAN-2004-1287	High	Secunia Advisory ID, SA13523, December 17, 2004 Debian Security Advisory DSA-623-1 nasm, January 4, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:004, January 6, 2005 Turbolinux Security Announcement, TLSA-24022005, February 24, 2005 **Fedora Update Notification, FEDORA-2005-322, April 18, 2005**
libexif libexif 0.6.9, 0.6.11	A vulnerability exists in the 'EXIF' library due to insufficient validation of 'EXIF' tag structure, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libe/libexif/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-17.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-300.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/libe/libexif/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this	LibEXIF Library EXIF Tag Structure Validation CAN-2005-0664	High	Ubuntu Security Notice USN-91-1, March 7, 2005 Fedora Update Notifications, FEDORA-2005-199 & 200, March 8, 2005 Gentoo Linux Security Advisory, GLSA 200503-17, March 12, 2005 RedHat Security Advisory, RHSA-2005:300-08, March 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:064, March 31, 2005 Debian Security Advisory, DSA 709-1, April 15, 2005 **SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005**

	vulnerability.			
libtiff.org LibTIFF 3.6.1 Avaya MN100 (All versions), Avaya Intuity LX (version 1.1-5.x), Avaya Modular Messaging MSS (All versions)	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ KDE: Update to version 3.3.2: http://kde.org/download/ Apple Mac OS X: http://www.apple.com/swupdates/ Gentoo: KDE kfax: http://www.gentoo.org/security/en/glsa/glsa-200412-17.xml Avaya: No solution but workarounds available at: http://support.avaya.com/elmodocs2/security/ASA-2005-002_RHSA-2004-577.pdf TurboLinux: http://www.turbolinux.com/update/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-354.html SGI: ftp://patches.sgi.com/support/free/security/advisories/	LibTIFF Buffer Overflows CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/ High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-2004:111, October 20 & 21, 2004 SuSE Security Announcement, SUSE-SA:2004:038, October 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, October 22, 2004 Slackware Security Advisory, SSA:2004-305-02, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:888, November 8, 2004 US-CERT Vulnerability Notes VU#687568 & VU#948752, December 1, 2004 Gentoo Linux Security Advisory, GLSA 200412-02, December 6, 2004 KDE Security Advisory, December 9, 2004 Apple Security Update SA-2004-12-02 Gentoo Security Advisory, GLSA 200412-17 / kfax, December 19, 2004 Avaya Advisory ASA-2005-002,

	SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.19 **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-021.html** Proofs of Concept exploits have been published.			January 5, 2005 Conectiva Linux Security Announcement, CLA-2005:914, January 6, 2005 Turbolinux Security Announcement, January 20, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005 RedHat Security Advisory, RHSA-2005:354-03, April 1, 2005 **RedHat Security Advisory, RHSA-2005:021-09, April 12, 2005**
Midnight Commander Midnight Commander 4.5.40-4.5.5.52, 4.5.54, 4.5.55	A buffer overflow vulnerability has been reported in the 'insert_text()' function due to insufficient bounds checking, which could let a malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Midnight Commander 'Insert_Text' Buffer Overflow CAN-2005-0763	High	Debian Security Advisory, DSA 698-1 , March 29, 2005 **Turbolinux Security Advisory, TLSA-2005-46, April 19, 2005**
moleSoftware GmbH VHCS 2.4 & possibly earlier versions	An input validation vulnerability has been reported due to insufficient validation of user-supplied data in HTTP POST requests, which could let a remote malicious user execute arbitrary SQL commands. Upgrades available at: http://isg.ee.ethz.ch/tools/postgrey/pub/postgrey-1.21.tar.gz Currently, we are not aware of any exploits for this vulnerability.	moleSoftware GmbH VHCS Input Validation CAN-2005-1128	High	Security Tracker Alert, 1013703, April 14, 2005
Monkey Monkey HTTP Daemon 0.1.4, 0.4-0.4.2, 0.5, 0.5.1, 0.6-0.6.3, 0.7.0- 0.7.2, 0.8-0.8.2, 0.9 .0	Two vulnerabilities have been reported: a Denial of Service vulnerability has been reported when handling certain requests due to an unspecified error; and a vulnerability has been reported in 'cgi.c' due to an unspecified error, which could let a malicious user execute arbitrary code. Upgrades available at: http://monkeyd.sourceforge.net/get_monkey.php?ver=17 Currently, we are not aware of any exploits for these vulnerabilities.	Monkey HTTP Daemon Denial of Service & Arbitrary Code Execution CAN-2005-1122 CAN-2005-1123	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14953, April 15, 2005
Multiple Vendors Apple Safari 1.2-1.2.3, RSS 2.0 pre-release; Omni Group OmniWeb 5.1	A vulnerability has been reported due to a failure to handle scripts securely, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.apple.com/safari/download/ A Proof of Concept exploit has been published.	Multiple Vendors Apple Safari Remote Code Execution CAN-2005-0976	High	Apple Security Advisory, APPLE-SA-2005-04-15, April 16, 2005

Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Debian: http://security.debian.org/pool/updates/main/p/perl/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 Debian Security Advisory, DSA 696-1 , March 22, 2005 **Turbolinux Security Advisory, TLSA-2005-45, April 19, 2005**
Multiple Vendors MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21.x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.54, 3.23.56, 3.23.58, 3.23.59, 4.0.0-4.0.15, 4.0.18, 4.0.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0, 2.1	A vulnerability exists in the 'GRANT' command due to a failure to ensure sufficient privileges, which could let a malicious user obtain unauthorized access. Upgrades available at: http://dev.mysql.com/downloads/mysql/4.0.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2004-611.html SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/m Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FedoraLegacy: http://download.fedoralegacy.org/fedora/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ **Debian:** **http://security.debian.org/pool/updates/main/m/mysql/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	MySQL Database Unauthorized GRANT Privilege CAN-2004-0957	Medium	Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Fedora Update Notification, FEDORA-2004-530, December 8, 2004 Turbolinux Security Announcement, February 17, 2005 Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005 Ubuntu Security Notice, USN-109-1 April 06, 2005 **Debian Security Advisory, DSA 707-1, April 13, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:070, April 13, 2005**

Multiple Vendors Concurrent Versions System (CVS) 1.x;Gentoo Linux; SuSE Linux 8.2, 9.0, 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9, 8, Open-Enterprise-Server 9.0, School-Server 1.0, SUSE CORE 9 for x86, UnitedLinux 1.0	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to an unspecified boundary error, which could let a remote malicious user potentially execute arbitrary code; a remote Denial of Service vulnerability was reported due to memory leaks and NULL pointer dereferences; an unspecified error was reported due to an arbitrary free (the impact was not specified), and several errors were reported in the contributed Perl scripts, which could let a remote malicious user execute arbitrary code. Update available at: https://ccvs.cvshome.org/servlets/ProjectDocumentList Gentoo: http://security.gentoo.org/glsa/glsa-200504-16.xml SuSE: ftp://ftp.suse.com/pub/suse/i Currently we are not aware of any exploits for these vulnerabilities.	CVS Multiple Vulnerabilities CAN-2005-0753	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200504-16, April 18, 2005 SuSE Security Announcement, SUSE-SA:2005:024, April 18, 2005 Secunia Advisory, SA14976, April 19, 2005
Multiple Vendors Daniel Stenberg curl 6.0-6.4, 6.5-6.5.2, 7.1, 7.1.1, 7.2, 7.2.1, 7.3, 7.4, 7.4.1, 7.10.1, 7.10.3-7.10.7, 7.12.1	A buffer overflow vulnerability exists in the Kerberos authentication code in the 'Curl_krb_kauth()' and 'krb4_auth()' functions and in the NT Lan Manager (NTLM) authentication in the 'Curl_input_ntlm()' function, which could let a remote malicious user execute arbitrary code. SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Updates available at: http://curl.haxx.se/download/curl-7.13.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200503-20.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-340.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows CAN-2005-0490	High	iDEFENSE Security Advisory , February 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:048, March 4, 2005 Gentoo Linux Security Advisory, GLSA 200503-20, March 16, 2005 Conectiva Linux Security Announcement, CLA-2005:940, March 21, 2005 ALTLinux Security Advisory, March 29, 2005 RedHat Security Advisory, RHSA-2005:340-09, April 5, 2005 **SGI Security Advisory, 20050403-01-U, April 15, 2005**
Multiple Vendors Gentoo Linux; rsnapshot filesystem snapshot utility 1.0.10, 1.1-1.1.6, 1.2	A vulnerability has been reported in the 'copy_symlink()' subroutine because file ownership is incorrectly changed on files pointed to by symlinks, which could let a malicious user manipulate file permissions. Upgrades available at: http://www.rsnapshot.org/	RSnapshot File Permission Manipulation CAN-2005-1064	Medium	rsnapshot Security Advisory 001, April 10, 2005

	downloads/rsnapshot-1.1.7.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200504-12.xml There is no exploit code required.			
Multiple Vendors GNOME GdkPixbuf 0.22 GTK GTK+ 2.4.14 RedHat Fedora Core3 RedHat Fedora Core2	A remote Denial of Service vulnerability has been reported due to a double free error in the BMP loader. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-344.html http://rhn.redhat.com/errata/RHSA-2005-343.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdk-pixbuf/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for this vulnerability.	GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service CAN-2005-0891	Low	Fedora Update Notifications, FEDORA-2005-265, 266, 267 & 268, March 30, 2005 RedHat Security Advisories, RHSA-2005:344-03 & RHSA-2005:343-03, April 1 & 4, 2005 Ubuntu Security Notice, USN-108-1 April 05, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:068 & 069, April 8, 2005 **SGI Security Advisory, 20050403-01-U, April 15, 2005**
Multiple Vendors RedHat Fedora Core3 & Core 2; Sylpheed Sylpheed 0.8, 0.8.11, 0.9.4-0.9.12, 0.9.99, 1.0 .0-1.0.3, 1.9-1.9.4	A buffer overflow vulnerability has been reported when handling email messages that contain attachments with MIME-encoded file names, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Sylpheed: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.4.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200504-02.xml **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Sylpheed MIME-Encoded Attachment Name Buffer Overflow CAN-2005-0926	High	Fedora Update Notifications, FEDORA-2005-263 & 264, March 29, 2005 Gentoo Linux Security Advisory, GLSA 200504-02, April 2, 2005 **Turbolinux Security Advisory, TLSA-2005-44, April 19, 2005**

Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2	A remote Denial of Service vulnerability has been reported when an unspecified Jabber file transfer request is handled. Upgrade available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-365.html** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	Gaim Jabber File Request Remote Denial of Service CAN-2005-0967	Low	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 **RedHat Security Advisory, RHSA-2005:365-06, April 12, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005**
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Ubuntu Linux 4.1 ppc, ia64, ia32	Two vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported due to a buffer overflow in the 'gaim_markup_strip_html()' function; and a vulnerability has been reported in the IRC protocol plug-in due to insufficient sanitization of the 'irc_msg' data, which could let a remote malicious user execute arbitrary code. Update available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-365.html** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities.	Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service & IRC Protocol Plug-in Arbitrary Code Execution CAN-2005-0965 CAN-2005-0966	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005 -298 & 299, April 5, 2005 Ubuntu Security Notice, USN-106-1 April 05, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 **RedHat Security Advisory, RHSA-2005:365-06, April 12, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005**
Multiple Vendors Todd Miller Sudo 1.5.6-1.5.9, 1.6-1.6.8	A vulnerability has been reported in VISudo due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	Sudo VISudo Insecure Temporary File Creation CAN-2005-1119	Medium	Security Focus, 13171, April 14,2005
Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Fedora Update Notifications, FEDORA-2005-236 & 237, March 18, 2005

	pool/updates/main/x/xli/ Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/** **TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.			Debian Security Advisory, DSA 695-1, March 21, 2005 **Turbolinux Security Advisory,** **TLSA-2005-43, April 19, 2005**
Paul Vixie Vixie Cron 4.1	A vulnerability has been reported due to insecure creation of temporary files when crontab is executed with the '-e' option, which could let a malicious user obtain sensitive information. **Fedora:** **http://download.fedora.redhat.com/** **pub/fedora/linux/core/updates/** There is no exploit code required; however, a Proof of Concept exploit script has been published.	Vixie Cron Crontab Information Disclosure CAN-2005-1038	Medium	Security Focus, 13024, April 6, 2005 **Fedora Update Notification,** **FEDORA-2005-320, April 15, 2005**
PHP Group PHP 4.3-4.3.10	A remote Denial of Service vulnerability has been reported when processing deeply nested EXIF IFD (Image File Directory) data. Upgrades available at: http://ca.php.net/get/php 4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/ glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/ en/ftp.php Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Nesting Remote Denial of Service CAN-2005-1043	Low	Security Focus, 13164, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005
PHP Group PHP 4.3-4.3.10	A vulnerability has been reported in the 'exif_process_IFD_TAG()' function when processing malformed IFD (Image File Directory) tags, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://ca.php.net/get/php 4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/ glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/ en/ftp.php Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Tag Integer Overflow CAN-2005-1042	High	Security Focus, 13163, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005

phpMyAdmin phpMyAdmin 2.0-2.0.5, 2.1- 2.1.2, 2.2, pre 1&pre2, rc1-rc3, 2.2.2-2.2.6, 2.3.1, 2.3.2, 2.4.0, 2.5.0-2.5.2, 2.5.4-2.5.7, 2.6.0pl1-2.6.0pl3, 2.6.1, pl1&pl3, 2.6.1 -rc1	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'convcharset' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.2-rc1.tar.gz?download Gentoo: http://security.gentoo.org/glsa/glsa-200504-08.xml **SUSE: ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required; however, a Proof of Concept exploit has been published.	phpMyAdmin 'convcharset' Cross-Site Scripting CAN-2005-0992	High	phpMyAdmin Security Announcement, PMASA-2005-3, April 3, 2005 Gentoo Linux Security Advisory, GLSA 200504-08, April 11, 2005 **SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005**
Postgrey Postgrey 1.16-1.18, 0.84-9.87	A format string vulnerability has been reported in the 'server.pm' module in the 'log' subroutine, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrades available at: http://isg.ee.ethz.ch/tools/postgrey/pub/postgrey-1.21.tar.gz Currently, we are not aware of any exploits for this vulnerability.	Postgrey Format String CAN-2005-1127	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14958, April 15, 2005
Salim Gasmi GLD 1.0-1.4	Several vulnerabilities have been reported: multiple buffer overflow vulnerabilities were reported in 'server.c' in the 'HandleChild' function, which could let a remote malicious user execute arbitrary code; and several format string vulnerabilities were reported in the 'cnf.c' file in the 'ErrorLog' function, which could let a remote malicious user execute arbitrary code with root privileges. Upgrades available at: http://www.gasmi.net/down/gld-1.5.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200504-10.xml A Proof of Concept exploit script has been published for the format string vulnerability.	Salim Gasmi GLD Buffer Overflows & Format Strings CAN-2005-1099 CAN-2005-1100	High	INetCop Security Advisory, #2005-0x82-026, April 11, 2005 Gentoo Linux Security Advisory, GLSA 200504-10, April 13, 2005
Sumus Sumus Game Server 0.2.2	A buffer overflow vulnerability has been reported in the 'RespondeHTTPPendiente()' function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Sumus Game Server Remote Buffer Overflow CAN-2005-1110	High	Security Tracker Alert, 1013717, April 14, 2005
Sun Microsystems, Inc. Solaris 7.0, 7.0 _x86, 8.0, 8.0 _x86, 9.0, 9.0 _x86	A vulnerability has been reported in the 'libgss' library because an unprivileged user can loan their own Generic Security Service Application Program Interface (GSS-API) which could lead to elevated privileges. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57734-1 Currently, we are not aware of any exploits for this vulnerability.	Sun Solaris libgss Elevated Privileges CAN-2005-1124	Medium	Sun(sm) Alert Notification, 57734, April 14, 2005
Sun Microsystems, Inc. Solaris 8.0, _x86, 9.0, _x86	A vulnerability has been reported due to an unspecified error, which could let a malicious user hijack non-privileged ports. Patches available at: http://sunsolve.sun.com/search/	Sun Solaris Network Port Hijacking	Medium	Sun(sm) Alert Notification, 57766 , April 18, 2005

	document.do?assetkey= 1-26-57766-1 Currently we are not aware of any exploits for this vulnerability.			
Wilmer van der Gaast Axel prior to 1.0b	A buffer overflow vulnerability has been reported in 'conn.c' when processing HTTP redirection messages, which could let a remote malicious user execute arbitrary code. Update available at: http://wilmer.gaast.net/ downloads/axel-1.0b.tar.gz Debian: http://security.debian.org/pool/ updates/main/a/axel/ Gentoo: http://www.gentoo.org/security/ en/glsa/glsa-200504-09.xml Currently, we are not aware of any exploits for this vulnerability.	Wilmer van der Gaast Axel 'Conn.c' Remote Buffer Overflow CAN-2005-0390	High	Security Tracker Alert, 1013709, April 14, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
All4WWW All4WWW-Homepagecreator 1.0 a	A vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'site' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	All4WWW-HomePageCreator 'Index.PHP' Arbitrary Code Execution CAN-2005-1117	High	Secunia Advisory: SA14972, April 15, 2005
Ariadne CMS 2.4	A vulnerability has been reported in the 'loader.php' file because the 'configs/ariadne.phtml' and 'configs/store.phtml' files are included relative to the 'araidne' variable without proper validation of the user-supplied variable, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Ariadne CMS Arbitrary Code Execution CAN-2005-1181	High	Security Tracker Alert,1013721, April 15, 2005
CityPost Image Cropper/Resizer 52	A Cross-Site Scripting vulnerability has been reported in the 'image-editor-52' script due to insufficient validation of the several variables, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CityPost Image Cropper/Resizer Cross-Site Scripting	High	sNKenjoi's Security Advisory, April 18, 2005
CityPost LNKX 52	A Cross-Site Scripting vulnerability has been reported in thee 'message.php' script due to insufficient validation of the 'msg' parameter, which could let a remote malicious user execute arbitrary HTML and script code.	CityPost PHP LNKX Cross-Site Scripting	High	sNKenjoi's Security Advisory, April 18, 2005

	No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.			
CityPost Simple PHP Upload 53	A Cross-Site Scripting vulnerability has been reported in the 'simple-upload-53.php' script due to insufficient validation of the 'message' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CityPost Simple PHP Upload Cross-Site Scripting	High	sNKenjoi's Security Advisory, April 18, 2005
Computer Associates BrightStor ARCServe Backup for Windows 9.0.1, 11.0, 11.1, 11.1 (All), (Client) 11.1, (Eng-All) 9.01, (Eng-Cli) 9.01, (NoEng-All) 9.01, (NoEng-Cli) 9.01, 64 bit 9.0.1, 64 bit 11.0, 64 bit 11.1, BrightStor Enterprise Backup 10.0, 10.5, BrightStor Enterprise Backup for Windows 64 bit 10.5	A buffer overflow vulnerability has been reported in the 'option' field due to a boundary error when receiving certain agent requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Updates available at: http://supportconnect.ca.com/sc/solcenter/ **An exploit script has been published.**	Computer Associates BrightStor ARCserve Backup UniversalAgent Remote Buffer Overflow CAN-2005-1018	Low/ High (High if arbitrary code can be executed)	iDEFENSE Security Advisory, April 11, 2005 **Security Focus, 13102, April 13, 2005**
Datenbank Datenbank Module for phpbb	Several vulnerabilities have been reported; a vulnerability has been reported in 'Mod.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability has been reported in 'Mod.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Datenbank PHPBB Module Remote 'Mod.PHP' SQL Injection & Cross-Site Scripting CAN-2005-1170 CAN-2005-1171	High	Bugtraq, 396048, April 16, 2005
eGroupWare eGroupWare 1.0.1, 1.0.6	A vulnerability has been reported because when an email with an attachment is composed, but not sent, then the attachment is sent to the next person the user emails, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	EGroupWare EMail Attachment Information Disclosure CAN-2005-1129	Medium	Secunia Advisory, SA14940, April 13, 2005
eGroupWare eGroupWare 1.0-1.0.3, 1.0.6	Multiple unspecified vulnerabilities have been fixed in the latest upgrade. The impact was not specified. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=78745 Currently we are not aware of any exploits for these vulnerabilities.	eGroupWare Multiple Vulnerabilities	Not Specified	Security Focus, 13213, April 18, 2005

F5 BigIP 9.0.2-9.0.4	An undisclosed vulnerability has been reported in the F5 BIG-IP user interface when a user is simultaneously logged into the web user interface with multiple clients. The impact was not specified. Update available at: http://tech.f5.com/home/bigip-next/solutions/gui/sol4369.html There is no exploit code required.	F5 BIG-IP User Interface	Not Specified	Security Focus,13240, April 19, 2005
Francisco Burzi PHP-Nuke 7.6	An HTTP response splitting vulnerability has been reported due to insufficient sanitization of the 'forwarder' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Francisco Burzi PHP-Nuke 'Forwarder' Parameter HTTP Response Splitting CAN-2005-1180	High	Dcrab 's Security Advisory, April 16, 2005
GNU GOCR Optical Character Recognition Utility 0.3.2, 0.3.4, 0.37, 0.39, 0.40	Several vulnerabilities have been reported: an integer overflow vulnerability was reported in the 'readpgm()' function that uses netpbm library when reading a specially crafted PNM, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability was reported in the 'readpgm()' function that doesn't use the netpbm library when reading a specially crafted PNM, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	GOCR 'ReadPGM' Remote Integer Overflows CAN-2005-1141 CAN-2005-1142	High	Overflow.pl Security Advisory #1, April 15, 2005
Gregory DEMAR Coppermine Photo Gallery 1.0 RC3, 1.1 beta 2, 1.1 .0, 1.2, 1.2.1, 1.2.2 b, 1.3	A vulnerability has been reported in the 'include/init.inc.php' script due to insufficient sanitization of user-supplied input before written in log files, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Coppermine Photo Gallery 'include/init.inc.php' HTML Injection CAN-2005-1172	High	Bugtraq, 396080, April 18, 2005
IBM iSeries AS400	A vulnerability has been reported in the POP3 service during authentication, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	IBM iSeries AS400 POP3 Server Remote Information Disclosure CAN-2005-1133	Medium	Securiteam, April 17, 2005
IBM Lotus Domino 6.0-6.0.3, 6.5.0-6.5.3	A buffer overflow vulnerability has been reported due to the way malformed HTTP POST requests are handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrade information available at: http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21202431 Currently we are not aware of any exploits for this vulnerability.	IBM Lotus Domino Server Malformed POST Request Remote Buffer Overflow CAN-2005-1101	Low/ High (High if arbitrary code can be executed)	Next Generation Insight Security Research (NGS Software) Advisory, April 12, 2005

IBM OS/400 5.x	A remote Denial of Service vulnerability has been reported in the IRC service when processing malformed data. Patch information available at: http://www-1.ibm.com/support/docview.wss?uid=nas29afd3991f5f290b086256fdb0053b293 Currently we are not aware of any exploits for this vulnerability.	IBM OS/400 Incoming Remote Command Denial of Service CAN-2005-1182	Low	Secunia Advisory, SA14970, April 18,2005
IBM Websphere Application Server 5.0, 5.0.1, 5.0.2 .1-5.0.2 .9, 5.0.2, 5.1.0.2-5.1.0.5, 5.1, 5.1.1-5.1.1 .3, 6.0	A vulnerability has been reported due to a failure to properly handle various requests under certain circumstances, which could let a remote malicious user obtain JSP source code. Workaround available at: http://publib.boulder.ibm.com/infocenter/ws60help/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/rtrb_jspsource.html There is no exploit code required; however, a Proof of Concept exploit has been published.	IBM WebSphere Application Server JSP Source Code Disclosure CAN-2005-1112	Medium	Security Tracker Alert,1013697, April 13, 2005
Kerio Technologies MailServer prior to 6.0.9	A remote Denial of Service vulnerability has been reported when a malicious user submits a specially crafted email message. Update available at: www.kerio.com/kms_home.htm Currently we are not aware of any exploits for this vulnerability.	Kerio MailServer WebMail Remote Denial of Service CAN-2005-1138	Low	Security Tracker Alert, 1013708, April 14, 2005
LG M4300, U8120, U8200, U8210	A remote Denial of Service vulnerability has been reported when processing a malicious MIDI file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	LG U8120 Mobile Phone MIDI File Remote Denial of Service CAN-2005-1132	Low	Security Focus, 13154, April 13, 2005
Matt Kruse CalendarScript 3.20, 3.21	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'calendar.pl' script due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported because a remote malicious user can submit an invalid calendar name to determine the installation path; a vulnerability was reported (version 3.21) when a remote malicious user submits a certain URL that causes sensitive information and debug information to be disclosed; and a vulnerability was reported (version 3.21) in the 'username' parameter because HTML code is not removed. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	CalendarScript Cross-Site Scripting & Information Disclosure CAN-2005-1145 CAN-2005-1146 CAN-2005-1147 CAN-2005-1148	Medium/ High (High if arbitrary code can be executed)	Security Tracker Alert ID: 1013705, April 14, 2005
Mozilla.org Mozilla Browser 1.0-1.0.2, 1.1-1.7.6, Firefox 0.8-0.10.1, 1.0.1, 1.0.2	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a	Mozilla Suite / Firefox Multiple Vulnerabilities CAN-2005-0752 CAN-2005-1153 CAN-2005-1154	High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005 Gentoo Linux Security Advisory, GLSA

	remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-18.xml There is no exploit code required.	CAN-2005-1155 CAN-2005-1156 CAN-2005-1157 CAN-2005-1158 CAN-2005-1159 CAN-2005-1160		200504-18, April 19, 2005 US-CERT VU#973309
Multiple Vendors Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2; K-Meleon K-Meleon 0.9; Netscape 7.2; **K-Meleon 0.9**	A vulnerability has been reported in the javascript implementation due to improper parsing of lamba list regular expressions, which could a remote malicious user obtain sensitive information. The vendor has issued a fix, available via CVS. There is no exploit code required; however, a Proof of Concept exploit has been published.	Mozilla Suite/Firefox JavaScript Lambda Information Disclosure CAN-2005-0989	Medium	Security Tracker Alert, 1013635, April 4, 2005 **Security Focus, 12988, April 16, 2005**
Multiple Vendors Linux kernel test12, 2.4-2.4.30, 2.6 .10, 2.6 -test1-test11, 2.6-2.6.11; Microsoft Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows 98SE, Windows NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT	A remote Denial of Service vulnerability has been reported when an active TCP session stream encounters an erroneous TCP acknowledgement number. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Multiple Vendor TCP Session Acknowledgement Number Remote Denial of Service CAN-2005-1184	Low	Security Focus, 13215, April 18, 2005

Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Windows Server 2003 Datacenter Edition, SP1, 2003 Datacenter Edition 64-bit, SP1, Windows Server 2003 Enterprise Edition, SP1, Windows Server 2003 Enterprise Edition 64-bit, SP1, Windows Server 2003 Enterprise x64 Edition, 2003 Standard Edition SP1				
Multiple Vendors See US-CERT VU#222750 for complete list	Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) do not adequately validate ICMP error messages, which could let a remote malicious user cause a Denial of Service. Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml IBM: ftp://aix.software.ibm.com/aix/efixes/security/icmp_efix.tar.Z RedHat: http://rhn.redhat.com/errata/ Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service CAN-2004-1060 CAN-2004-0790 CAN-2004-0791	Low	US-CERT VU#222750
Multiple Vendors Squid Web Proxy Cache 2.3, STABLE2, STABLE4-STABLE7, 2.5, STABLE1, STABLE3-STABLE9	A remote Denial of Service vulnerability has been reported when a malicious user prematurely aborts a connection during a PUT or POST request. Patches available at: http://www1.uk.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-post.patch Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ There is no exploit code required.	Squid Proxy Aborted Connection Remote Denial of Service CAN-2005-0718	Low	Security Focus, 13166, April 14, 2005
mvnForum mvnForum 1.0 RC4	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however,a Proof of Concept exploit has been published.	MVNForum Search Cross-Site Scripting CAN-2005-1183	High	Security Focus, 13213, April 18,2005
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability was reported in the CREATE FUNCTION command that could let an authenticated user gain mysql user privileges on the target system and permit the user to execute arbitrary code. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html Gentoo:	MySQL CREATE FUNCTION Remote Code Execution Vulnerability CAN-2005-0709	High	Security Tracker Alert ID: 1013415, March 11, 2005 Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005 Ubuntu Security Notice, USN-96-1 March 16, 2005

	http://security.gentoo.org/glsa/glsa-200503-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-334.html SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Debian: http://security.debian.org/pool/updates/main/m/mysql/** A Proof of Concept exploit has been published.		Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:019, March 24, 2005 RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Conectiva Linux Security Announcement, CLA-2005:946, April 4, 2005 **Debian Security Advisory, DSA 707-1 , April 13, 2005**

MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability has been reported that could let local malicious users gain escalated privileges. This is because the "CREATE TEMPORARY TABLE" command can create insecure temporary files. The vulnerabilities have been fixed in version 4.0.24 (when available): http://dev.mysql.com/downloads/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-334.html SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Debian: http://security.debian.org/pool/updates/main/m/mysql/** A Proof of Concept exploit has been published.	MySQL Escalated Privilege Vulnerabilities CAN-2005-0711	Medium	Secunia SA14547, March 11, 2005 Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005 Ubuntu Security Notice, USN-96-1 March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:019, March 24, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Conectiva Linux Security Announcement, CLA-2005:946, April 4, 2005 **Debian Security Advisory, DSA 707-1 , April 13, 2005**

MySQL AB MySQL 4.0.23, and 4.1.10 and prior	An input validation vulnerability was reported in udf_init() that could let an authenticated user with certain privileges execute arbitrary library functions on the target system. The udf_init() function in 'sql_udf.cc' does not properly validate directory names. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-334.html SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Debian:** **http://security.debian.org/pool/updates/main/m/mysql/** A Proof of Concept exploit has been published.	MySQL udf_init() Path Validation Vulnerability CAN-2005-0710	High	Security Tracker Alert ID: 1013414, March 11, 2005 Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005 Ubuntu Security Notice, USN-96-1 March 16, 2005 SUSE Security Announcement, SUSE-SA:2005:019, March 24, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Conectiva Linux Security Announcement, CLA-2005:946, April 4, 2005 **Debian Security Advisory, DSA 707-1 , April 13, 2005**
myWebland myBloggie 2.1.1	A vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	MyBloggie Arbitrary Code Execution CAN-2005-1140	High	Security Focus, 13192, April 15, 2005
NashTech EasyPHPCalendar	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in the 'index.php' script due to insufficient validation of the 'yr' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported in the 'popup.php' script due to an invalid 'ev' parameter value, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing.	EasyPHPCalendar Cross-Site Scripting & Information Disclosure CAN-2005-1143 CAN-2005-1144	Medium/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013704, April 14, 2005

	A Proof of Concept exploit has been published.			
Opera Software Opera Web Browser 8 Beta 3	A vulnerability has been reported due to a design error when using first-generation vetted digital certificates, which could lead to a false sense of security. No workaround or patch available at time of publishing. There is no exploit code required.	Opera SSL Security Feature False Sense of Security CAN-2005-1139	Medium	Security Focus, 13176, April 14, 2005
Oracle Corporation Oracle Application Server 10g, Enterprise Edition, Personal Edition, Standard Edition, Oracle8i Database Enterprise Edition, Standard Edition, Oracle9i Application Server, Oracle9i Database Enterprise Edition, Database Standard Edition	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary SQL code. Update information available at: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf Proofs of Concept exploits have been published.	Oracle Database Multiple SQL Injection	High	Security Focus 13144, April 12, 2005 US-CERT VU#982109
Oracle Corporation Oracle Application Server 10g, Collaboration Suite Release 2, Database 8.x, Database Server 10g, E-Business Suite 11i, Enterprise Manager 10.x, 9.x, Oracle9i Application Server, Oracle9i Database Enterprise Edition, Oracle9i Database Standard Edition, PeopleSoft EnterpriseOne Applications 8.x, PeopleSoft OneWorldXe/ERP8 Applications	Several vulnerabilities have been reported in the Change Data Capture, Data Pump, Intermedia, Authentication, Database SSL Library, Internet Directory, Spatial, XML Database, XDK, HTML database, and Oracle HTTP Server components, which could let a remote malicious user obtain database information, modify database information, and cause Denial of Service. Update information available at: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf Currently we are not aware of any exploits for these vulnerabilities.	Oracle Products Multiple Unspecified Vulnerabilities	Low/ Medium (Medium if information can be obtained or modified)	Secunia Advisory, SA14935, April 13, 2005
Oracle Corporation Oracle Forms versions 3.0 up to 10g	A vulnerability has been reported in the 'Query/Where' feature due to insufficient sanitization of user-supplied data, which could let a remote malicious user inject arbitrary SQL code. Update information available at: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf There is no exploit code required.	Oracle Applications 'Query/Where' Feature SQL Injection CAN-2005-1178	High	Securiteam, April 13, 2005
Oracle Corporation Oracle10g Application Server 10.1.0.2, Oracle10g Enterprise Edition 10.1.0.2, Oracle10g Personal Edition 10.1.0.2, Oracle10g Standard Edition 10.1.0.2	A buffer overflow vulnerability has been reported in the 'MDSYS.MD2.SDO_CODE_SIZE' procedure, which could let a remote malicious user execute arbitrary code. Update information available at: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf A Proof of Concept exploit script has been published.	Oracle Database 'MDSYS.MD2.SDO _CODE_SIZE' Buffer Overflow CAN-2004-1774	High	Security Focus, 13145, April 13, 2005
PHP Group PHP 4.3.6-4.3.9, 5.0 candidate 1-canidate 3, 5.0 .0-5.0.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'pack()' function, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the 'unpack()' function, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'safe_mode' when executing commands, which could let a remote	PHP Multiple Remote Vulnerabilities CAN-2004-1018 CAN-2004-1063 CAN-2004-1064 CAN-2004-1019 CAN-2004-1020 CAN-2004-1065	Medium/ High (High if arbitrary code can be executed)	Bugtraq, December 16, 2004 Conectiva Linux Security Announcement, CLA-2005:915, January 13, 2005 Red Hat, Advisory:

	malicious user bypass the security restrictions; a vulnerability exists in 'safe_mode' combined with certain implementations of 'realpath(),' which could let a remote malicious user bypass security restrictions; a vulnerability exists in 'realpath()' because filenames are truncated; a vulnerability exists in the 'unserialize()' function, which could let a remote malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists in the 'shmop_write()' function, which may result in an attempt to write to an out-of-bounds memory location; a vulnerability exists in the 'addslashes()' function because '\0' if not escaped correctly; a vulnerability exists in the 'exif_read_data()' function when a long sectionname is used, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in 'magic_quotes_gpc,' which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.php.net/downloads.php **Mandrake: http://www.mandrakesecure.net/en/ftp.php** Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-031.html SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Apple: http://www.apple.com/support/downloads/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ There is no exploit code required; however, a Proof of Concept exploit script has been published.	RHSA-2005:031-08, January 19, 2005 SUSE Security Announcement, SUSE-SA:2005:002, January 17, 2005 Ubuntu Security Notice, USN-66-1, January 20, 2005 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005 Ubuntu Security Notice, USN-99-1 March 18, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005**

PHP Group PHP prior to 5.0.4	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Slackware: ftp://ftp.slackware.com/pub/slackware/ **Debian: http://security.debian.org/pool/updates/main/p/php3/** **SUSE: ftp://ftp.SUSE.com/pub/SUSE** **Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities.	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1 April 05, 2005 Slackware Security Advisory, SSA:2005-095-01, April 6, 2005 **Debian Security Advisory, DSA 708-1, April 15, 2005** **SUSE Security Announcement, SUSE-SA:2005:023, April 15, 2005** **Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005**
phpBB Group phpBB 1.0 .0, 1.2.0, 1.2.1, 1.4 .0-1.4.2, 1.4.4, 2.0 .0, 2.0 RC1-RC4, 2.0 Beta 1, 2.0.1-2.0.13	A vulnerability has been reported in the Knowledge Base Module due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL or obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	phpBB Knowledge Base SQL Injection & Information Disclosure	High	Bugtraq, 396098, April 18, 2005
phpBB2 phpBB2 Plus 1.5, 1.52	Cross-Site Scripting vulnerabilities have been reported in 'GroupCP.php,' 'Indexphp,' 'Portal.php,' 'ViewForum.php,' and 'ViewTopic.php,' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPBB2 Plus Cross-Site Scripting Vulnerabilities CAN-2005-1113	High	Dcrab 's Security Advisory, April 13, 2005
Pinnacle Cart Pinnacle Cart	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'pg' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Pinnacle Cart 'Index.PHP' Cross-Site Scripting CAN-2005-1130	High	Secunia Advisory, SA14924, April 13, 2005
S9Y Serendipity 0.3-0.8	A vulnerability has been reported in the 'exit.php' script due to insufficient validation of the 'url_id' and 'entry_id' parameters, which could let a remote	Serendipity 'exit.php' Input Validation	High	ADZ Security Team Advisory, April 13, 2005

	malicious user execute arbitrary SQL code. Upgrades available at: http://www.s9y.org/12.html An exploit script has been published.	CAN-2005-1134		
Smartor Photo Album 2.0.53	Several vulnerabilities have been reported: an SQL injection vulnerability has been reported in 'Album_Search.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user inject arbitrary SQL code; and Cross-Site Scripting vulnerabilities have been reported in 'Album_Cat.PHP,' and 'Album_Comment.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Smartor PHPBB Photo Album Module SQL Injection & Cross-Site Scripting CAN-2005-1114 CAN-2005-1115	High	Security Focus, 13155, April 13, 2005
sphpBlog sphpBlog 0.4.0	Several vulnerabilities have been reported: a vulnerability was reported because the password.txt and config.txt files are stored under the web document root, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported in 'sb_functions.php' which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	SPHPBlog Information Disclosures CAN-2005-1136 CAN-2005-1137	Medium	Waraxe Advisory, April 13, 2005
sphpBlog sphpBlog 0.4.0	A Cross-Site Scripting vulnerability has been reported in 'Search.php' due to insufficient satiation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	SPHPBlog 'Search.PHP' Cross-Site Scripting CAN-2005-1135	High	Security Focus, 13170, April 14, 2005
Sun Microsystems, Inc. OpenOffice 1.1.4, 2.0 Beta	A vulnerability has been reported due to a heap overflow when a specially crafted malformed '.doc' file is opened, which could lead to a Denial of Service or execution of arbitrary code. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-13.xml** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any	OpenOffice Malformed Document Remote Heap Overflow CAN-2005-0941	Low/ High (High if arbitrary code can be executed)	Security Focus, 13092, April 11, 2005 **Fedora Update Notification, FEDORA-2005-316, April 13, 2005** **Gentoo Linux Security Advisory, GLSA 200504-13, April 15, 2005** **SUSE Security Announcement, SUSE-SA:2005:025, April 19, 2005**

	exploits for this vulnerability.			
Sun Microsystems, Inc. JavaMail 1.3.2	A Directory Traversal vulnerability has been reported in the 'MimeBodyPart.getFileName' method due to insufficient validation, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Sun JavaMail 'MimeBodyPart. getFileName' Directory Traversal CAN-2005-1105	Medium	Bugtraq, 395584, April 12, 2005
Veritas Software i3 FocalPoint Server 7.1	A vulnerability has been reported due to an unspecified error. The impact was also not specified. Patch available at: http://seer.support.veritas.com/docs/276119.htm Currently we are not aware of any exploits for this vulnerability.	Veritas i3 FocalPoint Server Unspecified Error CAN-2005-1131	Not Specified	Security Tracker Alert, 1013694, April 13, 2005
Xerox WorkCentre 32 Color 01.02.077.1, 01.02.058.4, 01.02.053.1, 01.00.060, 1.2.81, WorkCentre 40 Color 01.02.65.1, 01.02.077.1, 01.02.058.4, 01.02.053.1, 01.00.060, 1.2.81, WorkCentre M165 8.47.33.008. 8.47.30.000, 6.47.33.008, 6.47.30.000, WorkCentre M175 8.47.33.008, 8.47.30.000, 6.47.33.008, 6.47.30.000, WorkCentre M35 4.97.20.025, 4.84.16.000, 2.97.20.032, 2.28.11.000, 2.028.11.000, 4.97.20 .032, WorkCentre M45 4.97.20.025, 4.84.16.000, 2.97.20.032, 2.28.11.000, 4.97.20 .032, WorkCentre M55 4.97.20.025, 4.84.16.000, 2.97.20.032, 2.28.11.000, 4.97.20 .032, WorkCentre Pro 165 7.47.33.008, 7.47.30.000, WorkCentre Pro 175 7.47.33.008, 7.47.30.000, WorkCentre Pro 35 3.97.20.032, 3.028.11.000, WorkCentre Pro 45 3.97.20.032, 3.028.11.000, WorkCentre Pro 55 3.97.20.032, 3.028.11.000, WorkCentre Pro 65 1.001.02.084, 1.001.00.060, WorkCentre Pro 75 1.001.02.084, 1.001.00.060, WorkCentre Pro 90 1.001.02.084, 1.001.00.060, WorkCentre Pro Color 2128 0.001.04.044, Pro Color 2636 0.001.04.044, Pro Color 3545 0.001.04.044	A vulnerability has been reported in the SNMP functionality and the Web Server software, which could let a remote malicious user bypass authentication. Upgrades available at: http://www.xerox.com/downloads/usa/en/c/cert_P21_WCP_WebUI_Patch.zip Currently we are not aware of any exploits for this vulnerability.	Xerox MicroServer SNMP Authentication Bypass CAN-2005-1179	Medium	Xerox Security Bulletin, XRX05-005, April 12, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have

published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
April 18, 2005	amap-5.0.tar.gz	N/A	A next-generation scanning tool that allows you to identify the applications that are running on a specific port. It does this by connecting to the port(s) and sending trigger packets.
April 18, 2005	includer10.pl.txt includer10exec.pl.txt	No	Exploit scripts for the The Includer Remote File Include vulnerability.
April 18, 2005	kismet-2005-04-R1.tar.gz	N/A	Kismet is an 802.11 layer 2 wireless network sniffer that can sniff 802.11b, 802.11a, and 802.11g traffic.
April 18, 2005	msjet.c	No	Exploit for the Microsoft Jet Database Remote Code Execution Vulnerability.
April 18, 2005	ong_bak.c	Yes	Script that exploits the Linux Kernel Bluetooth Signed Buffer Index vulnerability.
April 18, 2005	p2pShareSpy.txt	No	Exploit for the Rebrand P2P Share Spy Information Disclosure Vulnerability.
April 18, 2005	pmSoftwareSimpleWebBufferOverflowPoC.pl	No	Perl script that exploits the PMSoftware Simple Web Server Remote Buffer Overflow vulnerability.
April 18, 2005	sash.c	No	Proof of Concept exploit for the sash 3.7 buffer overflow vulnerability.
April 18, 2005	storm.c	No	Proof of Concept exploit for the Multiple Vendor TCP Session Acknowledgement Number Denial of Service vulnerability.
April 17, 2005	23laeon.c.txt aeon02a.pl.txt	No	Exploit for the Aeon 0.2a and below vulnerability.
April 17, 2005	aiodio_read.c	No	Exploit for the Linux Kernel Asynchronous Input/Output Local Denial of Service vulnerability.
April 17, 2005	argo.c	No	Script that exploits the ArGoSoft FTP Server 'DELE' Command Remote Buffer Overflow vulnerability.
April 17, 2005	ftpNow2614.c	No	Script that exploits the Network-Client.com FTP Now Local Information Disclosure Vulnerability.
April 17, 2005	getdataBack.c	No	Script that exploits the Runtime GetDataBack for NTFS Local Information Disclosure Vulnerability.
April 17, 2005	mailenable_EHLO_DoS.pl	No	Perl script that exploits the MailEnable IMAP 'LOGIN' Command Buffer Overflow Vulnerability.
April 17, 2005	maxthon_arbitrary_read-write.html.txt	Yes	Exploit example for the GNU Maxthon Security ID Disclosure Vulnerability.
April 17, 2005	nokia_mms_gateway_vuln.txt	No	Exploit URLS for the Nokia MMS "Terminal Gateway" Login Bypass vulnerability.
April 17, 2005	ocean12_xss_and_sql_inj.txt	No	Example exploit URLs for the Ocean12 Membership Manager Pro Cross-Site Scripting and SQL Injection Vulnerability.
April 17, 2005	sco507nwprint.c	No	Script that exploits the SCO OpenServer NWPrint Command Buffer Overflow vulnerability.
April 17, 2005	Vixie_crontab_readfiles-exploit_and_advisory.txt	Yes	Proof of Concept exploit for the Vixie Cron Crontab Information Disclosure vulnerability.
April 15, 2005	libsafe-PoC.c	No	Proof of Concept exploit for the Libsafe Multi-threaded Process Security Bypass vulnerability.
April 14, 2005	netv-locsbof.c netv-remhbof.c	No	Exploits for the BakBone NetVault Buffer Overflows Permit Remote Code Execution vulnerability.
April 14, 2005	xsumus.c	No	Exploit for the Sumus Game Server Remote Buffer Overflow vulnerability.
April 14, 2005	yagerbof.zip	No	Exploit for the Yager Development Yager Game Buffer Overflow & Denial of Service vulnerabilities.
April 13, 2005	adz_serendipity.pl	Yes	Perl script that exploits the S9Y Serendipity Exit.PHP Input Validation vulnerability.

April 13, 2005	cabrightstor_uniagent.pm	Yes	Exploit for the Computer Associates BrightStor ARCserve Backup UniversalAgent Remote Buffer Overflow vulnerability.
April 13, 2005	lgfreeze.mid	No	Proof of Concept exploit for the LG U8120 Mobile Phone MIDI File Remote Denial of Service vulnerability.
April 13, 2005	ms05016.c windowsShellCodeExecPoC.cpp	Yes	Scripts that exploit the Microsoft Windows Shell Remote Code Execution Vulnerability.
April 13, 2005	oracle_sql_poc	Yes	Proofs of Concept exploits for the Oracle Database Multiple SQL Injection vulnerabilities.
April 12, 2005	0x82-meOw_linuxer_forever.c	Yes	Proof of Concept exploit for the Salim Gasmi Salim Gasmi GLD Buffer Overflow & Format String vulnerabilities.
April 12, 2005	oracle_bof_exp	Yes	Exploit for the Oracle Database MDSYS.MD2.SDO_CODE_SIZE Buffer Overflow vulnerability.
April 12, 2004	InternetExploiter2.zip	Yes	Proof of Concept exploit for the Microsoft Internet Explorer Remote Code Execution Vulnerability.

[back to top]

Trends

- **Russian hackers unite in organized criminal groups:** This year's e-Crime Congress revealed that while partnerships between law enforcement agencies are improving - witness the presence attendance of senior figures from the US Secret Service, FBI, Hong Kong Police and Russia's MVD General Miroshnikov - the level of online crime continues to expand as organized gangs cooperate across borders to steal and extort over the internet at unprecedented speed. Source: http://www.crime-research.org/news/18.04.2005/1159/ **Rootkits "Serious" Security Problem:** According to some security analysts, rootkits are now gaining popularity among virus writers. Rootkits can hide the existence of other malware on a computer by modifying file data, Windows registry keys, or active processes, all of which are used by malicious code detection software to spot worms, viruses, and spyware that's been installed on a PC. Source: http://informationweek.com/story/showArticle.jhtml?articleID=160900692. **Secure Sockets Layer security aiding online fraud:** The number of lower-security Secure Sockets Layer (SSL) certificates is increasing at twice the rate of the more secure organization-validated certificates - a situation some industry observers say could lead to increased online fraud. Domain-validated certificates, a lower-assurance form of certificate that many Certification Authorities (CAs) have begun issuing relatively recently, are one of several emerging controversies affecting Internet security and e-commerce. Source: http://www.techworld.com/security/news/index.cfm?NewsID=3468
- **Kelvir IM Worm Strikes Reuters**: Reuters Group was able to bring its instant messaging system back online early Friday morning, April 15, after an outbreak of the Kelvir worm led the company to shut down the system for most of Thursday. The London-based news and information provider detected the external worm on its network coming though a customer Internet portal mid-morning on Thursday and took the system down as a precaution, according to Reuters spokesperson Johnny Weir. After insuring there were proper filters in place, the IM system was made operational again on Friday. Source: http://www.pcworld.com/news/article/0,aid,120447,00.asp

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-Q	Win32 Worm	Stable	March 2004
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Mytob.C	Win32 Worm	Stable	March 2004
5	Bagle.BJ	Win32 Worm	Stable	January 2005
6	Netsky-D	Win32 Worm	Stable	March 2004
6	Netsky-Z	Win32 Worm	Stable	April 2004

7	Zafi-B	Win32 Worm	Stable	June 2004
7	Netsky-B	Win32 Worm	Stable	February 2004
8	Bagle-AU	Win32 Worm	Stable	October 2004
8	Sober-I	Win32 Worm	Stable	November 2004

Table Updated April 19, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Mytob**: The number of Mytob worm variants continues to grow, and spawning a record 40 variants since its appearance six weeks ago. Alfred Huger, senior director of engineering at Symantec's security response team, says the number of variants may result from numerous virus writers sharing the original source code and making their own changes. Source: http://www.securitypipeline.com/160701146
- **Sober**: A new Sober mass mailer worm is making its way around the Internet and tricking users into opening attachments with clever messages in both English and German, anti-virus companies warned Tuesday, April 19. W32.Sober.N@mm sends e-mail messages with the subject headers "I've_got your EMail on my_account!" and "FwD: Ich bin's nochmal" and carries attachments with names like your_text.zip, according to Helsinki security firm F-Secure. When opened, the attachment scans files on the infected computer to harvest e-mail addresses that enable the worm to spread. Source: http://www.nwfusion.com/news/2005/0419newsober.html

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
AdClicker-CJ		Trojan
Backdoor.Berpi		Trojan
BackDoor-CQO		Trojan
BackDoor-CQY		Trojan
Bancos.FC	Trj/Bancos.FC	Trojan
Dampig.A	FSCaller Hobbes.A SymbOS/Dampig.A	Symbian OS Worm
Del-472		Trojan
Downloader-YS		Trojan
Email-Worm.Win32.Bagle.pac		Win32 Worm
Gaobot.EYP	W32/Gaobot.EYP.worm	Win32 Worm
Kelvir.L	W32/Kelvir.L.worm	Win32 Worm
MultiDropper-MY		Trojan
Mytob.AR	W32/Mytob.AR.worm	Win32 Worm
Mytob.AT	W32/Mytob.AT.worm	Win32 Worm
SymbOS/Hobbes.a	Hobbes.A SymbOS.Hobbes.A SymbOS/Hobbes SYMBOS_HOBBES.A	Symbian OS Worm
SYMBOS_DAMPIG.B		Symbian OS Worm
SYMBOS_HOBBES.A		Symbian OS Worm
Troj/Agent-DI		Trojan
Troj/BagleDl-N		Trojan
Troj/Bancos-CD	Trojan-Spy.Win32.Bancos.cr TROJ_BANCOS.XZ	Trojan
Troj/Bancos-CG	TSPY_BANCOS.QL Trojan-Spy.Win32.Bancos.u	Trojan
Troj/Banker-CH	Trojan-Spy.Win32.Banker.oq	Trojan
Troj/Delbot-B		Trojan
Troj/Dloader-LR	Trojan-Downloader.Win32.Small.apv	Trojan
Troj/Dloader-LW	Trojan-Downloader.Win32.Delf.le	Trojan
Troj/DoomSend-A	Backdoor.Win32.Naninf.c	Trojan

TROJ_BAGLE.BH	W32/Bagle.dll.gen Win32.Glieder.T	Trojan
TROJ_STARTPAG.LA		Trojan
Trojan.Esteems		Trojan
Trojan.Mitglieder.P		Trojan
Trojan.Tooso.F		Trojan
Trojan.Tooso.G		Trojan
Trojan.Tooso.H		Trojan
Trojan-Dropper.Win32.Small.wy		Trojan
W32.Beagle.BN@mm		Win32 Worm
W32.Bufei		Win32 Worm
W32.Darro		Win32 Worm
W32.Kelvir.AA		Win32 Worm
W32.Kelvir.AB		Win32 Worm
W32.Kelvir.R		Win32 Worm
W32.Kelvir.S		Win32 Worm
W32.Kelvir.T		Win32 Worm
W32.Kelvir.U		Win32 Worm
W32.Kelvir.V		Win32 Worm
W32.Kelvir.W		Win32 Worm
W32.Kelvir.X		Win32 Worm
W32.Kelvir.Y		Win32 Worm
W32.Myfip.AC		Win32 Worm
W32.Mytob.AV@mm		Win32 Worm
W32.Mytob.AW@mm		Win32 Worm
W32.Picrate.B@mm		Win32 Worm
W32.Sinnaka.A@mm		Win32 Worm
W32.Spybot.NLX		Win32 Worm
W32.Spybot.NPS		Win32 Worm
W32.Spybot.NYT		Win32 Worm
W32/Agobot-RM	Backdoor.Win32.Agobot.abq	Win32 Worm
W32/Agobot-RN		Win32 Worm
W32/Bagle.br		Win32 Worm
W32/Codbot-K	Backdoor.Win32.Codbot.z W32/Gaobot.worm.gen.q W32.Randex	Win32 Worm
W32/Kelvir-I	Win32.Kelvir.I	Win32 Worm
W32/Kelvir-J	W32/Kelvir.worm.gen W32.Kelvir.T	Win32 Worm
W32/Mytob-AX	W32/Mytob.x@MM	Win32 Worm
W32/Mytob-BA	Net-Worm.Win32.Mytob.y	Win32 Worm
W32/Sdbot-XC	Backdoor.Win32.Agobot.abl W32/Sdbot.worm.gen.w	Win32 Worm
W32/Sdbot-XH		Win32 Worm
W32/Sober.o@MM	Email-Worm.Win32.VB.aj Sober.N W32.Sober.N@mm W32/Mytob.BU@mm W32/Sober-M W32/Sober.gen@MM Win32.Sober.M WORM_SOBER.N	Win32 Worm
W32/Sober-M		Win32 Worm
Win32.Bagle.BF		Win32 Worm
Win32.Glieder.T		Win32 Worm
Win32.Glieder.U		Win32 Worm
Win32.Glieder.V		Win32 Worm
Win32.Glieder.W		Win32 Worm
Win32.Glieder.X		Win32 Worm

Win32.Kelvir.F		Win32 Worm
Win32.Kelvir.H		Win32 Worm
Win32.Mytob Family		Win32 Worm
Win32.Mytob.AW		Win32 Worm
Win32.Mytob.BC		Win32 Worm
Win32.Ranck.FP		Win32 Worm
Win32.Rbot.CGH		Win32 Worm
Win32.Rbot.CGR		Win32 Worm
Win32.SillyDl.IQ		Win32 Worm
Win32.Slimad.C		Win32 Worm
Win32.Slinbot.ADX		Win32 Worm
WORM_BAGLE.BH	W32.Beagle.BN@mm W32/Bagle Win32.Bagle!generic	Win32 Worm
WORM_BAGLE.BI	W32/Bagle	Win32 Worm
WORM_KELVIR.N		Win32 Worm
WORM_KELVIR.O	W32.Kelvir Win32.Kelvir.F	Win32 Worm
WORM_KELVIR.P	Win32.Kelvir.I	Win32 Worm
WORM_KELVIR.Q		Win32 Worm
WORM_KELVIR.R	W32.Kelvir.P	Win32 Worm
WORM_KELVIR.T		Win32 Worm
WORM_KELVIR.U		Win32 Worm
WORM_KELVIR.V		Win32 Worm
WORM_MYTOB.AM	Net-Worm.Win32.Mytob.x W32.Mytob.AF@mm W32.Mytob.AM@mm W32/Mytob-AB W32/Mytob.AU@mm W32/Mytob.gen@MM Win32.Mytob.AJ Win32/Mytob.Z@mm	Win32 Worm
WORM_MYTOB.AT	W32.Mytob.AP@mm W32/Mytob Win32.Mytob.AK Win32/Mytob.W@mm	Win32 Worm
WORM_MYTOB.AY		Win32 Worm
WORM_MYTOB.BB	W32.Mytob.AF@mm W32/Mytob W32/Mytob.BN@mm Win32.Mytob.BB	Win32 Worm
WORM_MYTOB.BD	W32.Mytob.AR@mm W32/Mytob W32/Mytob.BL@mm	Win32 Worm
WORM_MYTOB.BF	W32.Mytob.AH@mm W32/Mytob W32/Mytob.BM@mm	Win32 Worm
WORM_MYTOB.BG	W32.Mytob.AF@mm W32/Mytob.BN@mm Win32.Mytob.BB	Win32 Worm
WORM_MYTOB.BH	W32.Mytob.AU@mm W32/Mytob W32/Mytob.BJ@mm	Win32 Worm
WORM_MYTOB.BH	W32.Mytob.AU@mm W32/Mytob.BJ@mm	Win32 Worm
WORM_MYTOB.BK	W32.Mytob.AS@mm W32/Mytob W32/Mytob.BP@mm Win32.Mytob.BC	Win32 Worm
WORM_MYTOB.BL	W32.Mytob.AS@mm W32/Mytob	Win32 Worm
WORM_MYTOB.BM		Win32 Worm
WORM_MYTOB.BQ		Win32 Worm
WORM_MYTOB.BR		Win32 Worm

WORM_MYTOB.BS		Win32 Worm
WORM_MYTOB.BU	DcomRpc.exploit*2 W32.Mydoom.gen@mm W32/Mydoom W32/Mytob.BV@mm	Win32 Worm
WORM_MYTOB.BW		Win32 Worm
WORM_MYTOB.BX		Win32 Worm
WORM_MYTOB.BY		Win32 Worm
WORM_SDBOT.BLL		Win32 Worm
WORM_SOBER.M	Trojan.Ascetic.B W32/Sober-M Win32.Sober.M	Win32 Worm

[back to top]

Last updated April 20, 2005